GRIFFIN KEY ATTRIBUTES

1. Griffin is a framework to provide a permanent, multinationally-developed, managed and resourced capability that enables the exchange of information between the classified networks of participating nations. It encompasses necessary infrastructure, connectivity, applications, services, management and governance.

2. Griffin enables the interconnection of different 'Communities of Interest' (COIs) which are cryptographically isolated using nationally accredited devices to provide the required confidentiality.

3. Establishment of different COIs requires additional cryptographic and network management equipment and security devices. Each COI requires duplicated equipment to provide separation and confidentiality of information.

4. The reach of Griffin is dependent on the 'reach' of each nation's classified network to its lower levels of command. The goal is to enable information sharing capability across all levels of command.

5. All nations who participate on Griffin contribute, materially and in-kind, to the development, operation and management of the capability.

6. Entry Criteria for a participating nation to operate on Griffin are:

    a. Interconnection of national classified (SECRET) networks via nationally managed security devices – the connection of stand-alone terminals not connected to national systems is not permitted.
    b. Nations will agree and implement one cryptographic equipment standard
    c. The Griffin communications backbone will consist of the US Defense Information Systems Network (DISN) and nationally-provided bearers.
    d. Each COI will require a separate MOU to meet national legal and security policy requirements and constraints. These MOUs should be similar and based on a commonly agreed security and information exchange standard (template).

7. Griffin is supported by Directory Services that provide different address lists for each COI. A 'Releasability/Classification Label' must be attached to each 'transaction' to ensure an originator will only be able to exchange information with other authorized users in the same community. Nations may be a member of several COIs at the same time.

8. An architectural approach for the implementation of coalition networks and their associated applications will be adopted. The Combined Communications Electronics Board (CCEB) will lead the development of allied and coalition network architectures in collaboration and/or association with participating nations and organizations. This will enable more timely and cost effective implementation of information sharing networks. This, along with the standardization of applications

will increase the usability of systems to operators, while also decreasing the cost of ownership through the use of common or standardized equipment, shared infrastructure, reduced training, better logistics support and ease of implementation.

9. Griffin provides a permanent information sharing capability. At the same time, other less permanent or Lead Nation-provided information exchange capabilities will almost always be required to allow the exchange of information to 'less-trusted' coalition partners, or when security restrictions will not permit the exchange of 'richer applications' (as a current example CHAT or COP) between nationally classified systems.

10. The Single Services (especially the AUSCANNZUKUS Navies) and other organizations (such as the Multinational Interoperability Program - MIP) have been very successful in developing multinational information exchange capabilities or effective gateways at the tactical level of command. These efforts are complementary to and are essential elements to enable the exchange of information across the strategic-operational-tactical continuum.

11. Griffin is Sponsored by the MIC, Enabled by the CCEB and Implemented by individual Nations.

Agreed Terminology

Griffin - Griffin is a framework that enables the exchange of information between classified national C2 networks of participating nations on multiple domains.

Domain – A common environment where participants can exchange information that is protected from intrusion from non-participants.

Security Domain – A domain where information can be exchanged at an agreed upon and assured security level.

Communities of Interest - A group of users within a domain that share a common interest, objective, security arrangement or goal.

Network Convergence - The process of separate networks merging into one.

Tier 1 - A coalition capability or application that can be accessed from a national C2 network.

Tier 2 - A coalition capability or application that is not integrated/connected to national C2 systems and can be accessed from a stand-alone C2 system.

Boundary Protection Service (BPS) - BPS provides the security to protect national C2 systems when connecting coalition networks

Griffin Capability

Connecting National Secure C2 Networks